3GPP TSG SA WG3 Security – SA3#28 **S3-030236**
6 - 9 May 2003
Berlin, Germany

Title: **UE-Initiated Tunneling with L2TP/IPSec**

Source: **Nokia**
Agenda item: **7.11**
Document for: **Discussion and decision**

1 Introduction

SA2 informs in their LS on 'impacts on the UE of UE-Initiated Tunnelling' (*TDoc S3-030189*) to SA3#28 that they are currently working on tunneling issues for interworking between 3GPP system and WLAN systems. As a working assumption, SA2 is currently only considering UE-Initiated tunneling. This contribution discusses the role of UE-initiated tunneling and proposes L2TP/IPSec (RFC 3193) as a one potential solution.

2 Discussion

UE-initiated tunneling can be decoupled from WLAN session set-up, and user choice can be taken into account. As the tunnel starts from the UE, it is possible to achieve a higher level of security than in UE-transparent tunneling (i.e. purely network based), because cleartext user data packets are not accessible to WLAN AN or the visited PLMN.

The other end of the end-to-end tunnel is still open in SA2, but one candidate is the Packet Data Gateway (PDGW). However, it has been agreed in SA2 that for non-roaming case, UE-Initiated tunnel has the remote tunnel endpoint in Home PDGW.

TS 23.234 v1.7.0 (draft), states that

- tunnel establishment is not coupled to WLAN session establishment,
- UE may establish several tunnels in order to access several IP network simultaneously,
- the actual IP network selection is performed as part of the establishment of each tunnel.

To meet the SA2 requirements, the tunneling protocol should have the following properties:

- Tunnel establishment should include subscriber authentication, tunnel authorization, including using legacy authentication, i.e. username/password and W-APN (WLAN APN).
- IP network selection by user choice. This could be realized for example by selecting a different W-APN for each IP network. For instance, the W-APN could be resolved to a PDGW IP address using DNS by the UE, or the W-APN could be included as a parameter in signaling.
- IP address and other IP configuration from the remote IP network
- Encryption and integrity protection for both tunnel establishment and user data packets
- IPv6 transport in order to support IMS even if the WLAN AN or other intermediate networks were IPv4-only
- Based on available standards, protocol details agreeable in 3GPP
- Supported in current legacy WLAN terminals, i.e. laptop operating systems
- Be capable of traversing NAPT (Network Address and Port Translation) boxes as they seem to be the legacy of WLAN IPv4 AN.

2.1 L2TP/IPSec

Virtual Private Network (VPN) techniques, such as IPsec tunnel mode or Layer 2 Tunneling Protocol (L2TP) over IPsec, are suitable candidates for the protocols. The protocol details should be specified up to stage 3 in 3GPP to enable interoperability in a multi-vendor environment.

L2TP over IPsec has the above-mentioned properties. As it is based on a tunneled Point-to-Point Protocol (PPP) session, it would provide roughly the same functionality as a GPRS PDP context. Any network layer protocol, including IPv4, IPv6 and X.25, can be transported over L2TP. All PPP legacy authentication methods can be supported. In addition to remote-access applications, a tight integration with IPsec allows L2TP to focus on tunneling applications and gives users the ability to optionally engage the IPsec portion with relative ease. For instance, L2TP over a private network may not require the additional security and overhead of IPsec, and so it can be turned off. However, in operating over the Internet when security is a must, IPsec may be easily deployed in a standardized manner.

Keys for tunnel establishment have to be obtained from WLAN authentication directly or other possibility is to utilize subscriber certificates. In both cases the IPsec IKE is needed, but this is FFS.

IPSec NAPT traversal functionality has been incorporated into many NAPTs. On top of that, IETF is working on a generic solution using UDP tunneling (*draft-ietf-ipsec-nat-t-ike-05.txt*, *draft-ietf-ipsec-udp-encaps-06.txt*). Earlier versions of these drafts have been already implemented in commercially available products.

2.1.1 L2TP_v3

It is also noted that there is a new L2TP version 3 coming (*draft-ietf-l2tpext-l2tp-base-07.txt*), which has been decoupled from PPP.

3 Proposal

It is proposed that SA3 uses L2TP/IPSec for a secure VPN solution for UE-initiated tunneling in 3GPP-WLAN interworking scenario 3 and takes under further investigation the related design details.